PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**Group Art Unit: 2137**
	)	
Harold VATER *et al.*	)	**Examiner: Z. Davis**
	)	
Serial Number: 09/700,656	)	***Attorney Docket*: VATE3001beu**
	)	
Filed: February 14, 2001	)	**Confirmation No.: 7577**

For: Access-Controlled Data Storage Medium

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Honorable Commissioner For Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

A response to a Notice of Non-Compliance is submitted concurrently herewith, but the response does not include any amendments.

This request is being filed with a notice of appeal.

The review is requested for the reasons stated on the attached sheets (no more than 5 pages are provided). I am the attorney or agent of record.

Respectfully submitted,
BACON & THOMAS, PLLC

Date: November 20, 2006

By: BENJAMIN E. URCIA
Registration No. 33,805

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500

REASONS FOR REQUESTING REVIEW OF THE FINAL REJECTION

(Attachment to Pre-Appeal Brief Request for Review)

Review of the final rejection of claims 26-33 and 42 is requested based on the following two errors made by the Examiner in the reasons for maintaining the rejections set forth in the attachment to the Advisory Action dated October 26, 2006:

1. The teaching in U.S. Patent No. 6,049,613 (Jakobsson) of a random number used to create a checksum for verifying processor operation is not, as alleged by the Examiner, suggestive of an " auxiliary function value ($f(Z)$) [that] was **previously determined** by execution of the one or more operations (f) with the auxiliary data (Z) as input data **in safe surroundings** and ***stored*** along with the auxiliary data (Z)"; and
2. The Jakobsson patent does not, as alleged by the Examiner, teach "combining the output data determined by execution of the one or more operations (f) with an auxiliary function value ($f(Z)$) **in order to *compensate* for the falsification of the input data**," as recited in claim 26, but to the contrary teaching combining output data with a random number to prevent cheating.

Claim 1 specifically recites the steps of:

- falsifying the input data by combination with auxiliary data (Z) before execution of one or more operations (f),
- combining the output data determined by execution of the one or more operations (f) with an auxiliary function value ($f(Z)$) in order to compensate for the falsification of the input data,
- wherein the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z),

According to the invention, input data is blinded by combination with Z before performing operations f. The output is then combined with $f(Z)$ to recover the input data (compensation

for the blinding or data falsification). Compensation is made possible because f has previously been determined to give $f(Z)$ when f is applied to Z.

According to the Examiner, Z and $f(Z)$ correspond to the random number generated during the Jakobsson verification process (as explained the last paragraph on the attachment to the Advisory Action). However, simply generating a random number, as taught by Jakobsson, will not enable the claimed compensation for data falsification. One can certainly falsify data by combining with a random number, but one cannot recover the original data without application of some additional functions that lead back to the number used to falsify the data. Since Jakobsson is not concerned with disguising data for later recover, but rather is concerned solely with verifying processor operation by parallel operations on a random number, Jakobsson does not require the claimed storage of an auxiliary function *and* data used to previously obtain that function.

The Examiner argues that one can generate random numbers and pre-store them. However, even if Jakobsson's random number were actually a pre-stored "pseudo-random" number, the result does not correspond to the claimed invention, in which the data Z used to disguise the input data is previously applied to functions f that result in an auxiliary function $f(Z)$ executed with functions f to achieve the compensation. **It is respectfully submitted that *pre-storing a random number* does not, as alleged by the Examiner, reasonably correspond to the claimed feature "*wherein the auxiliary function value (f(Z)) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z)*."** Pre-storing a random number is not even taught by Jakobsson and, even if it were taught, would not come close to suggesting the claimed invention.

According to the invention, two values Z and $f(Z)$ are stored so that they can later be used to disguise input data and operations while obtaining the same result as if the

undisguised operations had been performed on the undisguised data. In contrast, Jakobsson generates a random number which is combined with data to generate a checksum in order to verify processor operation and prevent cheating. There is **no possible need** in Jakobsson to calculate an auxiliary function value $f(Z)$ in safe surroundings and to store even one number, much less $f(Z)$ with Z as claimed, and the result does not achieve the compensation of the claimed invention. A number that is calculated by applying a predetermined function to a predetermined value cannot be said to be random or even "pseudo-random" as suggested by the Examiner, and thus the claimed invention is contrary to what is taught by Jakobsson.

While the "blinding" steps of Jakobsson could be considered to "falsify" input data by combination with auxiliary data, Jakobsson does not attempt to calculate the claimed auxiliary function such that f(Z) compensates for f(input data combined with Z) in order to recreate f(input data). Jakobsson has no need to do so because Jakobsson's re-encryption is used solely to compare the operations of parallel processors and determine whether the processors are functioning correctly or cheating. In fact, the outcome of Jakobsson's combination of processors is not f(input data combined with Z), *i.e.*, an operation on falsified input data, but rather the original input data that has been "permuted" (the order of the original data has been changed).

The reason why Jakobsson does not attempt to falsify input data and then obtain the same result as if the input data had not been falsified is that, in the method of Jakobsson, the data itself, which consists of **election results**, is **not secret**. In fact, it **must** not be changed. The only secret is who voted for whom, *i.e.*, the order of results. The purpose of Jakobsson's "blinding" operations is to compare blinded results, as opposed to obtaining the same results by performing a falsified operation f(Z) on falsified data as would have been achieved by performing an original operation f on original data, which has the effect of making it impossible to recreate the original operation f. As a result, following Jakobsson's "re-encryption" operation, *i.e.*, the modulo or data combining operations, the results of the data combining operations from different processors are compared, and the process terminates *without compensation for the re-encryption operation*. If

no error is found, the operations of the processors are simply considered to be valid, while if an error is found, then the operations are considered to be invalid. In either case, the result of the data combining operations are of no further use, and there is no need for any sort of compensation.

Basically, the process of Jakobsson operates as follows:

- a processor of a first "blinding" section, such as processor 20 shown in Fig. 5, first permutes the input (changes the order) and then "re-encrypts" the data (combines it with other numbers, which may be random).
- The results are immediately compared or another "blinding" section is applied and the results are used to "prove" partial correctness of the output (see col. 7, lines 29-47).
- If correct, the permutated results are output. If not, one of the processors or sets of processors is eliminated as un-trustworthy and permutation of the election results continued.

This process does not refer to an auxiliary function value that was ***previously*** determined by execution of the one or more operations with the auxiliary data as input data in ***safe surroundings*** and stored along with the auxiliary data. Instead, it is only necessary in Jakobsson that each of the processors to be compared perform predetermined functions. The data or values to be combined do not need to be predetermined.

In the process of Jakobsson, *any* combination of modulo and other operations will work, so long as the results are comparable. The results do not matter, so long as they are the same for each processor or set of processors. If the results are different, then one of the processors or sets of processors is not to be trusted. This is completely contrary to the claimed invention, in which the result of applying function f to the falsified input data (Z combined with input data) must be the same as the result of applying the original functions *f* to the original input data. Accordingly, reversal and withdrawal of the rejection of claims 26-33 and 42 in view of the Jakobsson patent is requested.